DEPARTMENT OF THE AIR FORCE
HQ AIR INTELLIGENCE AGENCY

AIR INTELLIGENCE AGENCY INSTRUCTION 33-116

21 January 1999

Communication and Information

HEADQUARTERS AIR INTELLIGENCE AGENCY NETWORKS INFRASTRUCTURE AND COMPUTER SYSTEMS MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AIA WWW site at: http://pdo.pdc.aia.af.mil/library/pubs.

OPR: 690 CSS/IPM (Mr. George Wynkoop)

Certified by: 690 IOG/CC (Col Gary L. Davis)

Pages: 8

Distribution: F

This instruction implements AFPD 33-1, Command, Control, Communications, and Computer (C4) Systems, AFI 33-112, Computer Systems Management, and AFI 33-115 V1, Network Management. It provides standard processes and procedures and sets forth responsibilities for effective management and control of HQ Air Intelligence Agency (AIA) networks, systems, and architectures. This instruction also provides guidance to ensure standardized, interoperable, secure, network systems capable of effective support to the information operations mission of AIA. Within HQ AIA, there are computer networks operating at different security classification levels. These networks are critical resources, vital for HQ AIA units to effectively accomplish their missions. This instruction provides management guidance for these networks and associated hardware and software systems. This instruction applies to users of the networks within the HQ AIA directorates and major staff offices, the 690th Information Operations Group (690 IOG), the 67th Intelligence Wing (67 IW), and other units not covered under a service level agreement (SLA). The Directorate of Personnel (HQ AIA/DP) is authorized to maintain a separate unclassified local area network (LAN) because of its unique personnel systems requirements. Other collocated AIA and non-AIA organizations, such as the Air Force Information Warfare Center (AFIWC) and the Joint Command and Control Warfare Center (JC2WC) who operate separate networks interfacing with the HQ AIA networks will negotiate an SLA with the 690 IOG (see paragraph 4.3). In addition, if the 690 IOG supports any HQ AIA organization that has a requirement that is unique (for example, a unique functional system such as PC III) or exceeds the standard of service normally provided, they must negotiate an SLA with the 690 IOG for support of that particular requirement. This instruction does not apply to AIA-gained Air National Guard or Air Force Reserves units.

1. Networks. HQ AIA has three networks that provide worldwide desktop workstation connectivity between HQ AIA, the Department of Defense (DoD) Intelligence community, and other authorized activities. Each network operates at a different security classification level. The classification levels include:

1.1. Top Secret Sensitive Compartmented Information (TS/SCI) LAN. The TS/SCI LAN is accredited for information up to Top Secret SI/TK and provides access to two distinct wide area networks: the Joint Worldwide Intelligence Communications System (JWICS) and the National Security Agency Network (NSANet). The TS/SCI LAN also supports office automation and the Intelligence Data Handling System (IDHS).

1.2. Secret LAN. The Secret LAN is accredited for information up to Secret collateral and provides connectivity to the Secret Internet Protocol Routing Network (SIPRNet).

1.3. Unclassified LAN. The Unclassified LAN is accredited for unclassified information and provides connectivity to the Unclassified Internet Protocol Routing Network (NIPRNet), the Open Source Information System (OSIS) network, and the world wide web (www).

2. Network Management. Effective management of HQ AIA networks design, configuration, operation, and security is critical to ensure HQ AIA users can effectively perform their information operations missions. The 690 IOG is responsible for the overall management of HQ AIA networks, but effective network management requires the involvement of all using organizations. The 690 IOG establishes a Network Operations Working Group (NOWG) for each network.

3. Functions and Responsibilities of Management Levels:

3.1. The Commander (690 IOG/CC). The 690 IOG/CC is designated the HQ AIA Communications and Information Systems Officer (CSO). The CSO performs functions in concert with the base CSO duties outlined in AFI 33-103, Requirements Development and Processing, AFI 33-112 (the 668th Logistics Squadron [668 LS] performs functions according to AFI 33-112, paragraphs 6.1, 6.2, 6.3, 6.10, 6.12, 6.13, 10, 11, section C, and section E), AFI 33-115, and the command, control, communications, and computers (C4) systems planner duties outlined in AFI 33-104, Base-Level Planning and Implementation. In addition, the CSO:

3.1.1. Plans and implements HQ AIA target architectures according to AIAI 33-111, Preferred Hardware and Software Architecture.

3.1.2. Negotiates agreements, as required, with the local base communications squadron.

3.1.3. Manages the configuration management of networks. The CSO writes and implements a network configuration management plan and performs configuration management according to AIAI 33-106, Air Intelligence Agency Configuration Management.

3.2. Network Operations Working Group (NOWG). The NOWG is an action officer-level working group chaired by 690 IOG personnel appointed by the CSO. The working group meets on a regular basis to determine overall operational requirements and direction for their network. Each major functional user (for example, Directorate of Information Operations [HQ AIA/DO], Directorate of Logistics [HQ AIA/LG], Directorate of Financial Management [HQ AIA/FM], AFIWC, Cryptologic Systems Group [CPSG], 67 IW, etcetera), will appoint one NOWG representative with the authority to vote on behalf of their functional area. The NOWG:

3.2.1. Assesses the impact of proposed major network changes in relation to each representative's functional area business process. In this context, the NOWG reviews new user requirements and downward-directed programs that may have significant impact on network operational capability. The NOWG by majority vote, approves, disapproves, and, or prioritizes these requirements, as needed. Dissenting organizations may appeal NOWG decisions to the CSO for possible reconsid-

eration. The functional two-letter (for example, HQ AIA/LG, HQ AIA/FM, etcetera) or organizational equivalent approves the appeals before they are presented to the CSO.

3.2.2. Determines rank order of all unfunded requirements. The 690 IOG submits these requirements to HQ AIA/DO, who forwards the requirements to the HQ AIA Financial Working Group for funding consideration by the Financial Management Board (HQ AIA/FMB). However, these unfunded requirements are not in rank order in the HQ AIA/DO-sponsored funding priorities. The unfunded requirements remain as separate requirements. At the discretion of the FMB, any unfunded requirements may be entered into the AIA Corporate Process for funding consideration.

3.2.3. Advises the CSO on network operational requirements, ensuring the CSO is aware of mission, process, or business changes that may have a significant impact on network capability or drive baseline changes.

3.2.4. Advocates acquisition of resources to upgrade network operational capability.

3.2.5. Assists the 690 IOG in preparing their respective functional areas for network upgrades, procedural changes, and technology insertions. This includes the identification of training requirements and needed capabilities.

3.2.6. Works with the 690 IOG Configuration Management Office (CMO) to develop and approve a standard configuration for systems connected to the LAN.

3.2.7. Works with the 690 IOG Systems Integration Management Office (SIMO) to ensure systems integration and compliance with Air Force and DoD standards and direction.

4. Network Operations Responsibilities. The daily operations and maintenance of HQ AIA networks are distributed responsibilities. The 690 IOG provides overall day-to-day management of network operations and maintenance. Within functional areas, workgroup managers (WGM) provide day-to-day operational support to users.

4.1. Workgroup Manager. The WGM is the initial level of response to problems, and the customer's first source for help. WGMs are certified before they perform WGM duties. Certification indicates the WGM possesses the skills and knowledge necessary to function effectively as a WGM. The 690 IOG certifies WGMs using a standardized Certification Task List (CTL) that defines WGM responsibilities. The 690 IOG develops the CTL and reflects Air Force direction as stated in AFI 33-115. If required, 690 IOG provides training to WGMs for certification. Each functional area appoints at least one WGM. The functional area ensures a sufficient number of WGMs are appointed to provide adequate support to their customer base.

NOTE:

Small functional areas, such as Office of the Surgeon General (HQ AIA/SG), may seek a WGM that resides in a larger functional area to support them.

4.2. 690 IOG:

4.2.1. Manages day-to-day operations and maintenance of HQ AIA networks. The group runs the HQ AIA Network Operations Center (NOC) and performs functional system administrator duties for all HQ AIA networks not under an SLA.

4.2.2. Provides operational and maintenance services that are outside the responsibilities of the WGM for all hardware and software standard configurations approved by the NOWG and the 690 IOG CMO. Support for approved requirements that are not part of the standard configuration is addressed on a case-by-case basis and may require an SLA for system implementation and, or support. Do not implement approved requirements until adequate life-cycle logistics support is identified and funded for that requirement to ensure the system is properly implemented and maintained.

4.3. Service Level Agreements (SLA). An SLA defines roles and responsibilities for network operations and services. AFI 33-115 defines SLAs and shows their proper format. The 690 IOG negotiates an SLA with an organization that is requesting support for network services or has a requirement that is unique or exceeds the standard of service provided. The SLA makes clear the services the 690 IOG provides and the requesting organization's responsibilities, including any necessary funding. In order to maintain network security and ensure effective configuration management, a signed SLA must be in effect before establishing interface between the HQ AIA networks and the networks maintained by other collocated AIA and, or non-AIA organizations. An annual review of the SLA will be conducted by the 690 IOG and the organization. Negotiate and document changes as required. If an SLA does not exist for organizations with networks that have established interfaces with the HQ AIA network, an SLA must be negotiated and signed immediately.

5. Computer Systems Management. In order to provide effective asset, security, and configuration management, strict control is required over hardware and software that operates on HQ AIA networks. Computer Systems Management is a distributed responsibility.

5.1. Network Focal Point. The 690 IOG acts as the focal point for network software and software license management.

5.2. Acquisition and Accountability. The 668 LS implements all actions regarding acquisition and accountability according to AFI 33-112 (including paragraphs 6.1, 6.2, 6.3, 6.10, 6.12, 6.13, 10, 11, sections C and E).

5.3. Organizational Computer Manager (OCM). Each major functional user appoints an OCM. In addition to the duties outlined in AFI 33-112, the OCM:

5.3.1. Acts as the requirements approval authority for the functional user.

5.3.2. Coordinates closely with the NOC, FSA, WGMs, equipment custodians (EC), and the IPMS office to ensure appropriate delivery and effective management of functional area computer systems and associated software.

5.3.3. Ensures adequate support (for example; funding, personnel, license tracking, installation, contract renewal, etcetera) is provided for approved hardware and software requirements used in their functional area that are not part of the standard configuration designated by the NOWG and the 690 IOG Configuration Management Office.

6. Computer Systems Acquisition. Do not purchase hardware or software without an approved AF Form 3215, C4 Systems Requirements Document, and a completed technical solution. Use the appropriate OCM address for delivery of all procurement actions (AF Form 9, Request for Purchase, IMPAC [International Merchant Purchase Authorization Card], etcetera). The appropriate EC ensures deliveries are inventoried and added to the IPMS.

7. Transfer or Removal of Computer Hardware or Software:

7.1. The NOC coordinates and approves the transfer or destruction of software.

7.2. The respective local security manager or the 67th Support Squadron Security Office (67 SPTS/SO) coordinates the transfer or removal of C4I equipment connected to a classified network (Secret or TS/SCI). The appropriate security accreditation packages are reviewed and updated as required.

JOHN R. BAKER, Brigadier General, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

References

Air Force:

AFPD 33-1, Command, Control, Communications, and Computer (C4) Systems

AFI 33-101, Communications and Information Management Guidance and Responsibilities

AFI 33-103, Requirements Development and Processing

AFI 33-104, Base-Level Planning and Implementation

AFI 33-112, Computer Systems Management

AFI 33-115, Network Management

Air Intelligence Agency:

AIAI 33-106, Air Intelligence Agency Configuration Management

AIAI 33-111, HQ AIA Preferred Hardware and Software Architecture

Department of Defense and Joint:

DoD 52001.R, Information Security Program

Joint DODIIS/Cryptologic SCI Information System Security Standards

Abbreviations and Acronyms

67 IW—67th Intelligence Wing

690 IOG—690th Information Operations Group

748th—748th Army Battalion

AIA—Air Intelligence Agency

AFI—Air Force Instruction

AFIWC—Air Force Information Warfare Center

C4I—Command, Control, Communications, Computers and Intelligence

CM—Configuration Management

CPSG—Cryptologic Systems Group

CSO—C4 Systems Officer

DoD—Department of Defense

EC—Equipment Custodian

ECO—Equipment Control Officer

FSA—Functional System Administrator

LAN—Local Area Network

IDHS—Intelligence Data Handling System

IPMS—Information Processing Management System

JWICS—Joint Worldwide Intelligence Communications System

NIPRNet—Nonclassified Internet Protocol Routing Network

NOC—Network Operations Center

NOWG—Network Operations Working Group

NSANet—The National Security Agency Network

OCM—Organizational Computer Manager

OSIS—Open Source Information System

SIPRNet—Secret Internet Protocol Routing Network

SLA—Service Level Agreement

Terms

Accreditation—The official authorization granted by the appropriate Designated Approving Authority (DAA), on a case-by-case basis, permitting the processing of an information system.

Command, Control, Communications, and Computer (C4) System—A C4 system is an integrated system of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communication designed to support a commander's exercise of command and control across the range of military operations.

C4 System Officer (CSO)—The person given responsibility for overall management of the AIA complex C4 systems.

Complex—The area known as Security Hill, Kelly Air Force Base, later to be part of the Lackland Air Force Base complex. It also encompasses areas connected to and managed under the AIA chartered LANs and or networks.

Configuration Management—A discipline applying technical and administrative direction and surveillance to:

(a) identify and document the functional and physical characteristics of C4 systems;

(b) to control changes of those characteristics; and

(c) record and report changes to processing and implementation status.

Functional Area—A HQ AIA Directorate, 67 IW, 690 IOG, or any unit directly using the HQ AIA Networks Infrastructure.

Information System—Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data and includes computer software, firmware, and hardware.

Local Area Network (LAN)—A LAN has the capability to provide local interoperability.

Network—A combination of information transfer resources devoted to the interconnection of two or more distinct devices, systems, or gateways.

Operation—Supports the user with day to day ability to access and process authorized information transferred or stored on the LANs and networks.

Organizational Computer Manager (OCM)—The person given responsibility for overall management of organizational C4 systems. In addition to the organizational head (that is; Director, Commander, etcetera), the person that approves organizational C4 requirements, signs the AF Form 3215 as the organizational representative, and manages and, or advises the organizational head on SLA issues and recertification.

System Security—The timely application of system security management and engineering principles throughout all phases.